SOC IMS: SOC-20110808-224190

Last Updated: 6/13/2012 3:05 AM

SOC Incident Management System

IMS User Contact:	(b) (6), (b) (7)(C)	**Restrict Access To:**	All IMS
Record Permissions Group:	All IMS Users	**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:		**Contact First Name:**	
Contact Role:		**Contact Office Phone:**	
Contact E-mail:		**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	SOC-20110808-224190	**Categorization:**	Incident
Date Record Created (UTC):	8/8/2011 6:06 PM	**Incident Time Zone:**	UTC - Coordinated Universal Time Zone (GMT)
Title:	ARC - Unauthorized Access		
Brief Description:	Compromised ARC system (b) (7)(E), . Possible SQL injection attack again (b) (7)(E) .		
Current Status:	Resolved	**Assigned To:**	ARC IRM ARC IRT ARC ITSM
Current Priority:	Low	**Also Notify:**	

CUI:	Maybe SBU Only	**Notify on Save:**	No
CUI Categories:			
Ok To Close:	No		

US CERT Reporting

Risk Rating:			
Information Impact:		**Functional Impact:**	
Recoverability:		**Attack Vectors:**	
Critical Service or System:		**Classified Incident:**	
Major Incident:		**High Value Assets (HVA):**	
Reportable to Congress:			
Observed Activity:		**Number of Records Impacted:**	
Location of Observed Activity:		**Number of Systems Impacted:**	
Actor Characterization:		**Number of Users Impacted:**	
Action Taken to Recover:		**Number of Files Impacted:**	

The fields below hold the US-CERT Reporting fields that were in force from October 1, 2015 through March 31, 2017. The are included here for reporting purposes only.

Functional Impact old:		**Informational Impacts old:**	
		Recoverability Impact old:	

Sensitive But Unclassified

Reason SBU is suspected to be involved:		**How SBU was disclosed:**	
SBU Media Format:		**SBU Media Format Medium:**	
Date & Time Incident Occurred:		**Date & Time of Discovery of SBU Loss:**	

Scope of SBU Exposure:		**SBU Data Elements Exposed:**	
Original Information Owner:		**Number of Individuals without the appropriate "Need to Know" for Information Associated with this Exposure:**	
Protection of SBU Data Elements:		**SBU Trade Secrets:**	
Law Enforcement or IG Notified about SBU:		**Time to Report:**	

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
No Records Found						

Related Incidents

Select Relationship:		**Relationship Description:**	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Incident Details

Time Incident Started:	8/8/2011 11:00 AM	**Time Incident Started (UTC):**	8/8/2011 11:00 AM
Time Incident Detected:	8/8/2011 11:00 AM	**Time Incident Detected (UTC):**	8/8/2011 11:00 AM
Center Affected by Incident:	ARC	**Overall Impact (reference):**	Moderate

US-CERT Category:	CAT 5 - Scans/Probes/Attempted Access	**Incident Subcategory:**	
US-CERT Tracking Number:	INC000000166870	**ESD Ticket #:**	
Resolution Status:	Concluded	**Malware Family:**	
		Highest level of access gained:	
Primary Method used to Identify Incident:	System Administrator		
Primary Attack Category:			
Primary Vulnerability Type:		**Lost or Stolen NASA Equipment:**	

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
(b) (7)(E)			ARC

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack
No Records Found			

Campaigns

Campaign Name:		**Reviewed By TVA:**	
Campaign Comment:		**Confirmed By TVA:**	
		Is APT:	

Indicators of Compromise

IOC Domain

FQDN	Do Sinkhole	Comment

No Records Found

IOC IP

IP Address	IP Block	Comment

No Records Found

IOC File

Filename	MD5 Hash	Comment

No Records Found

IOC Registry Key

Key Name	Key Value	Comment

No Records Found

IOC Email

Sender Email	Subject	Comment

No Records Found

IOC Detection

Name	Type	Comment

No Records Found

Root Cause Statement

The Root Cause Statement can be constructed from the following fields like so:

(b) (7)(E), (b) (2)

Root Cause Sources:		**Root Cause Categories:**	
Root Cause Methods:		**Root Cause Causes:**	
Root Cause Factors:		**Root Cause Objectives:**	

Reporting Organizations

Reporting Date (UTC)	Reporting Local Date	Reporting Local Time Zone	Reporting Notes	Reporting Number	Reporting Organization	Reporting Organization Contact

No Records Found

Impact of Incident

NASA Programs, Projects, and/or Operations:	Low	**People:**	Moderate

Data (at Rest or Transmission):	Low	**System:**	Low
Cost:	Low	**Sophistication / Nature of Attack:**	Low
Number of systems affected by this incident:	1	**Number of NASA Centers/ Facilities affected by this incident:**	
Number of accounts affected by this incident:	2-5	**Critical Infrastructure Impacted:**	No
Other Impacts:	Moderate		
Overall Impact:	Moderate -- Incident Considered Moderate if any of the Categories are rated Moderate but not High		

Containment Actions

Incident Containment System Action:	
Incident Containment Network Action:	

Recovery Actions

Incident Recovery System Action:	
Incident Recovery User Action:	

Recommendations

Root Cause:	(b) (7)(E)
Lessons Learned:	

Costs

Center (Hours):	8.00	**Center (Dollars):**	800.00
NASA SOC (Hours):		**NASA SOC (Dollars):**	
NASA NOC (Hours):		**NASA NOC (Dollars):**	

Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):	8	**Total Cost (Dollars):**	800
Description of Costs:			
System Down Time (Days):		**System Down Time (Hours):**	

Timeline

Date Record Opened (UTC):	8/8/2011 6:06 PM	**Date Record Confirmed (UTC):**	6/13/2012 4:33 AM
Date Record Contained (UTC):	8/17/2011 3:44 PM	**Date Record Resolved (UTC):**	8/17/2011 3:44 PM
Date Record Closed (UTC):			
Time in Open:	309.42		
Time in Confirmed:		**Time to Confirm:**	309.00
Time in Contained:		**Time to Contain:**	8.90
Time in Resolved:		**Time to Resolve:**	8.90
Time in Closed:		**Time to Close:**	
Number of Days to Resolve:	8.901		

Journal Entries

Entry	Entry Date	IMS User
US-Cert needs clarification of the following: - Credential disclosure. The SQL database associated with this bbs was dumped including password hashes. At least two of these hashes were cracked and posted online. 8/17/2011 - (b) (6), ARC - Using a publicly known vulnerability (b) (6), (b) (7)) which leveraged a flaw in the input validation of the (b) (7)(E), (b) (2) parameter on out of date vbulletin installs an attacker	8/17/2011 3:06 AM	(b) (6), (b)

was able to access the password hashes used by the vbulletin install via a SQL Injection attack. Two of the hashes obtained were posted online at (b) (7)(E), (b) (2) (also included by (b) (6), (b) in an early Journal entry) .

- There is no evidence this far that suggests a system compromise. The passwords obtained were only used for the bbs instance.

8/17/2011 - (b) (6), ARC - A disk image of the VMWare instance hosting this server was taken. Review of the image found no evidence that the underlying operating system had been compromised. The hashes/passwords obtained by the SQL Injection attack were only used to authenticate with the vbulletin webapp and could not be used to leverage further access to this or other NASA systems. The disclosure of the leveraged (b) (7)(E) ' vulnerability indicates it can be used to exploit latent vulnerabilities in the underlying database, but there is no evidence found that this was attempted or achieved.

8/16/2011 7:08 PM (b) (6),

SOC Ticket: SOC-20110808-224190
Date: 08/08/2011
IP: (b) (7)(E)
Hostname: (b) (7)(E)
User: (b) (6), (b)
Administrator: (b) (6), (b)
Sponsor: PEROT SYSTEMS
Code: PX
Network: Public
Root Cause (b) (7)(E), (b) (2)
Mitigation: (b) (7)(E)

Information: Review of the system image found no signs of system level access. A interview with the maintainer confirmed site contained no PII/SBU and was in the process of development before priorities were sidetracked leaving the site below current revision level for a small amount of time. It is unclear when the SQLi/credentials were compromised, but lack of source from the available logs suggest post 3 months. The previous site will be dropped and a new VM/webapp install will be vetted from scratch. Confirmed exposed credentials were only used on the vbulletin instance, and will now be considered lost and never reused in any fashion.

. Below are some notes from the information we have gathered so far: 8/10/2011 11:10 PM (b) (6),

- Web-app compromise (SQL injection). The vbulletin bbs system run from this site was out of date and vulnerable to publically released exploit code.
- Credential disclosure. The SQL database associated with this bbs was dumped including password hashes. At least two of these hashes were cracked and posted online.
- There is no evidence this far that suggests a system compromise. The

passwords obtained were only used for the bbs instance.
- We are tracking this incident via IMS ticket SOC-20110808-224190

Image has been taken of the suspended VM instance.

This appears to possibly be related to Ticket 224205 (opened later today) where this was cleaned:

8/8/2011 9:08 PM

(b) (6), (b)

(b) (7)(E)

Content:

Nasa Vulnerable to a public SQLi Exploit - Embarassing much?

Admin Username: (b)
Email: (b) (6), (b) (7)(C)
Hashed Password:
Salt: (b) (7)(E)

Admin Username: (b) (6),
Email: (b) (6), (b) (7)(C)
Hashed Password:
(b) (7)(E)

- If shit like this is vulnerable to public exploits, imagine whats vulnerable to private 0days :) -

[+] TriCk - TeaMp0isoN
[+] Shoutouts: iN^SaNe - Hex00010 - MLT

Twitter:
@TeaMp0isoN_

**NOTE: A joint #TeaMp0isoN & #Anonymous Operation is about to hit the interwebs soon **

This public URL indicates the (b) (7)(E) forum (as mentioned in the earlier journal) was compromised by "TeaMp0isoN" .. making it likely these two events are related:

http://tweetmeme.com/story/6007808536/teamp0ison-nasa-forum-is-vulnerable-sql-injection-admin-hacked-thn-the-hacker-news

TeaMp0isoN : NASA forum is Vulnerable SQL injection, Admin Hacked !TeaMp0isoN Hackers crew today Reveal on twitter that the discussion forum on NASA website at (b) (7)(E) is Vulnerable to SQL injection. The discussion Forum script is Powered by Vbulletin. According to hacker, He use Vbulletin 4.0.x => 4.1.3 (b) (7)(E) SQL injection

Vulnerability Exploit

On 8/8/2011 the Admin of (b) (7)(E) contacted ARC IT Security to report the running vbulletin bbs server had been compromised. The bbs server was taken down and the admin disabled the NIC interface of the system. (b) (7)(E) is VM instance. Admin has been contacted to create a snapshot image of the running instance for review.	8/8/2011 8:33 PM	(b) (6),

Attachment(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

History Log

View History Log